特 許 協 力 条 約

PCT

特許性に関する国際予備報告（特許協力条約第二章）

（法第12条、法施行規則第56条）
〔ＰＣＴ36条及びＰＣＴ規則70〕

出願人又は代理人の書類記号　YG200413PCT	今後の手続きについては、様式ＰＣＴ／ＩＰＥＡ／４１６を参照すること。	
国際出願番号 ＰＣＴ／ＪＰ２００４／０１６５８９	国際出願日（日.月.年）　０９．１１．２００４	優先日（日.月.年）　１０．１１．２００３
国際特許分類（ＩＰＣ）Int.Cl. ***G09C1/00*** (2006.01), ***H04L9/10*** (2006.01), ***H04L9/32*** (2006.01)		
出願人（氏名又は名称） 独立行政法人科学技術振興機構		

1．この報告書は、ＰＣＴ35条に基づきこの国際予備審査機関で作成された国際予備審査報告である。
法施行規則第57条（ＰＣＴ36条）の規定に従い送付する。

2．この国際予備審査報告は、この表紙を含めて全部で　4　ページからなる。

3．この報告には次の附属物件も添付されている。

a．☑ 附属書類は全部で　3　ページである。

☑ 補正されて、この報告の基礎とされた及び／又はこの国際予備審査機関が認めた訂正を含む明細書、請求の範囲及び／又は図面の用紙（ＰＣＴ規則70.16及び実施細則第607号参照）

☐ 第Ｉ欄４．及び補充欄に示したように、出願時における国際出願の開示の範囲を超えた補正を含むものとこの国際予備審査機関が認定した差替え用紙

b．☐ 電子媒体は全部で＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿（電子媒体の種類、数を示す）。
配列表に関する補充欄に示すように、電子形式による配列表又は配列表に関連するテーブルを含む。
（実施細則第802号参照）

4．この国際予備審査報告は、次の内容を含む。

☑ 第Ｉ欄　国際予備審査報告の基礎
☐ 第Ⅱ欄　優先権
☐ 第Ⅲ欄　新規性、進歩性又は産業上の利用可能性についての国際予備審査報告の不作成
☐ 第Ⅳ欄　発明の単一性の欠如
☑ 第Ⅴ欄　ＰＣＴ35条(2)に規定する新規性、進歩性又は産業上の利用可能性についての見解、それを裏付けるための文献及び説明
☐ 第Ⅵ欄　ある種の引用文献
☐ 第Ⅶ欄　国際出願の不備
☐ 第Ⅷ欄　国際出願に対する意見

国際予備審査の請求書を受理した日 ０２．０９．２００５	国際予備審査報告を作成した日 １７．１１．２００５
名称及びあて先 日本国特許庁（ＩＰＥＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　５Ｓ　４２２９ 青木　重徳 電話番号　０３－３５８１－１１０１　内線　３５４６

様式ＰＣＴ／ＩＰＥＡ／４０９（表紙）（２００５年４月）

特許性に関する国際予備報告

国際出願番号 ＰＣＴ／ＪＰ２００４／０１６５８９

第Ⅰ欄　報告の基礎

1．言語に関し、この予備審査報告は以下のものを基礎とした。

☑ 出願時の言語による国際出願

☐ 出願時の言語から次の目的のための言語である＿＿＿＿＿＿ 語に翻訳された、この国際出願の翻訳文

- ☐ 国際調査（ＰＣＴ規則12.3(a)及び23.1(b)）
- ☐ 国際公開（ＰＣＴ規則12.4(a)）
- ☐ 国際予備審査（ＰＣＴ規則55.2(a)又は55.3(a)）

2．この報告は下記の出願書類を基礎とした。（法第6条（ＰＣＴ14条）の規定に基づく命令に応答するために提出された差替え用紙は、この報告において「出願時」とし、この報告に添付していない。）

☐ 出願時の国際出願書類

☑ 明細書

第＿＿＿１，３－１５＿＿＿ ページ、出願時に提出されたもの
第＿＿＿＿＿２＿＿＿＿＿ ページ*、０２．０９．２００５ 付けで国際予備審査機関が受理したもの
第＿＿＿＿＿＿＿＿＿＿ ページ*、＿＿＿＿＿＿ 付けで国際予備審査機関が受理したもの

☑ 請求の範囲

第＿＿＿１－３，５，６＿＿＿ 項、出願時に提出されたもの
第＿＿＿＿＿＿＿＿＿＿ 項*、ＰＣＴ１９条の規定に基づき補正されたもの
第＿＿＿＿＿４＿＿＿＿＿ 項*、０２．０９．２００５ 付けで国際予備審査機関が受理したもの
第＿＿＿＿＿＿＿＿＿＿ 項*、＿＿＿＿＿＿ 付けで国際予備審査機関が受理したもの

☑ 図面

第＿＿＿１－７＿＿＿ ~~ページ／~~図、出願時に提出されたもの
第＿＿＿＿＿＿＿＿＿＿ ページ／図*、＿＿＿＿＿＿ 付けで国際予備審査機関が受理したもの
第＿＿＿＿＿＿＿＿＿＿ ページ／図*、＿＿＿＿＿＿ 付けで国際予備審査機関が受理したもの

☐ 配列表又は関連するテーブル
配列表に関する補充欄を参照すること。

3．☐ 補正により、下記の書類が削除された。

- ☐ 明細書　第＿＿＿＿＿＿＿＿＿＿ ページ
- ☐ 請求の範囲　第＿＿＿＿＿＿＿＿＿＿ 項
- ☐ 図面　第＿＿＿＿＿＿＿＿＿＿ ページ／図
- ☐ 配列表（具体的に記載すること）＿＿＿＿＿＿＿＿＿＿
- ☐ 配列表に関連するテーブル（具体的に記載すること）＿＿＿＿＿＿＿＿＿＿

4．☐ この報告は、補充欄に示したように、この報告に添付されかつ以下に示した補正が出願時における開示の範囲を超えてされたものと認められるので、その補正がされなかったものとして作成した。（ＰＣＴ規則70.2(c)）

- ☐ 明細書　第＿＿＿＿＿＿＿＿＿＿ ページ
- ☐ 請求の範囲　第＿＿＿＿＿＿＿＿＿＿ 項
- ☐ 図面　第＿＿＿＿＿＿＿＿＿＿ ページ／図
- ☐ 配列表（具体的に記載すること）＿＿＿＿＿＿＿＿＿＿
- ☐ 配列表に関連するテーブル（具体的に記載すること）＿＿＿＿＿＿＿＿＿＿

＊ 4．に該当する場合、その用紙に "superseded" と記入されることがある。

特許性に関する国際予備報告

国際出願番号 ＰＣＴ／ＪＰ２００４／０１６５８９

第Ｖ欄　新規性、進歩性又は産業上の利用可能性についての法第12条（ＰＣＴ35条(2)）に定める見解、それを裏付ける文献及び説明

1．　見解

新規性（N）	請求の範囲	1－6	有
	請求の範囲		無
進歩性（ＩＳ）	請求の範囲		有
	請求の範囲	1－6	無
産業上の利用可能性（ＩＡ）	請求の範囲	1－6	有
	請求の範囲		無

2．　文献及び説明（ＰＣＴ規則70.7）

文献１：Anand Krishnamurthy, Yiyan Tang, Cathy Xu and Yuke Wang, "AN EFFICIENT IMPLEMENTATION OF MULTI-PRIME RSA ON DSP PROCESSOR", Proceedings 2003 IEEE International Conference on Multimedia and Expo, Volume 3 of 3, 2003.07.06-09, p.437-440

文献２：ＪＰ　７－２８７５１４　Ａ（フィリップス　エレクトロニクス　ネムローゼ　フェンノートシャップ），１９９５．１０．３１

文献３：ＪＰ　２００３－５１７６７１　Ａ（コーニンクレッカ　フィリップス　エレクトロニクス　エヌ　ヴィ），２００３．０５．２７

請求の範囲１－６に係る発明は、文献１、２及び３に記載されているものから、当業者にとって自明である。

文献１には、ＲＳＡアルゴリズムの約分演算を処理するにあたり、Montgomeryアルゴリズムを用いることで高能率な演算が可能であることを開示しており、この演算手法を１０２４ビットＲＳＡ署名演算としてＤＳＰ汎用プロセッサに実装し、実用可能な範囲内で署名操作を完了できる旨の実験結果が記載されている。

文献２には、特に第【００２３】，【００２４】段落において、秘密鍵などをＥＥＰＲＯＭに格納することで外部から読み出せないようにして、メッセージ署名をチップカードで実行可能とした技術が記載されており、署名されるべきメッセージが組み立てる必要のある任意のメッセージに従って予め決定された構造に従わないものである場合、メッセージの署名を禁止する手段を備えることが示唆されており、また、ＥＥＰＲＯＭに格納された秘密鍵の外部読み出せないようにする構成として、直接パスを設けないよう配線を工夫することは当業者にとって常套手段である。

加えて、プロセッサにて演算処理を行うにあたり、レジスタやゲート、カウンタ等の構成要素を用いることは文献３に記載されているように、当業者にとって常套手段である。

そして、各文献がいずれもプロセッサにおけるセキュリティ処理の実現を図る技術に

補充欄

いずれかの欄の大きさが足りない場合

第 Ｖ．２ 欄の続き

ついて記載したものである点を勘案すれば、文献１に記載されている汎用プロセッサによるＲＳＡアルゴリズムでの署名演算処理に、前記常套手段を考慮して文献２に記載されている鍵管理技術や署名の禁止処理を採用し、請求の範囲１－６に係る発明をなすことは当業者にとって自明なことである。

[0003] 本発明の目的は、汎用機能を持ち、なおかつ、セキュリティ機能(すなわち鍵データの安全保管とデジタル署名計算の高速化)も持つプロセッサの提供である。

課題を解決するための手段

[0004] 上述の目的を達成するために、本発明は、鍵データを格納した不揮発性メモリで構成される鍵レジスタと、該鍵レジスタに格納された鍵データを1ビットずつ参照するために、ビット位置を示す鍵カウンタと、デジタル署名に用いるダイジェスト・データを格納するダイジェスト・レジスタと、前記鍵カウンタにより参照された1ビットの鍵データが0のときは前記ダイジェスト・レジスタの内容を1、1のときは前記ダイジェスト・レジスタの内容をそのまま出力するゲートとを備え、前記鍵レジスタには全データを外部から読み取るパスは設けず、一般命令とともに、前記鍵レジスタ、前記鍵カウンタ、及び前記ダイジェスト・レジスタを操作して前記ダイジェスト・データからデジタル署名を求めるための複数の署名専用命令を有することを特徴とするセキュア・プロセッサである。

これにより、汎用機能を持ち、不揮発性メモリの鍵レジスタに格納した鍵データを直接的には読めないため、セキュリティ機能も持つプロセッサを提供することができる。

このプロセッサの走行モードとして、一般モードとセキュリティ・モードを有し、前記セキュリティ・モードを表示するセキュリティ・レジスタを備えるとともに、前記セキュリティ・モードをセットする一般命令及びリセットする署名専用命令を有し、前記一般命令は一般モードのときに有効となり、前記署名専用命令はセキュリティ・モードのときに有効となるとすることもできる。

[0005] 前記セキュリティ・モード設定命令は、前記セキュリティ・レジスタをセットすると同時に、前記鍵カウンタを1023に初期設定し、前記署名専用命令は、署名計算を鍵レジスタの1ビット分実行する命令の実行と同時に鍵カウンタをデクリメントして、順次ビットごとの署名計算が進行し、前記鍵カウンタが0のときのみにセキュリティ・モードをリセットする構成とし、一旦、デジタル署名の演算過程に入ると、終了するまで(鍵カウンタが0となるまで)、演算過程から抜けられず、演算過程の中間結果からプログラムにより鍵データを推定することを不可能としている。

前記ダイジェスト・レジスタに設定されたダイジェスト・データが16ビット毎に少なくとも1つの1を有することを検出する手段を備え、前記セキュリティ・モード設定命令は、16ビット

請求の範囲

[1] 鍵データを格納した不揮発性メモリで構成される鍵レジスタと、

該鍵レジスタに格納された鍵データを1ビットずつ参照するために、ビット位置を示す鍵カウンタと、

デジタル署名に用いるダイジェスト・データを格納するダイジェスト・レジスタと、

前記鍵カウンタにより参照された1ビットの鍵データが0のときは前記ダイジェスト・レジスタの内容を1、1のときは前記ダイジェスト・レジスタの内容をそのまま出力するゲートとを備え、

前記鍵レジスタには全データを外部から読み取るパスは設けず、

一般命令とともに、前記鍵レジスタ、前記鍵カウンタ、及び前記ダイジェスト・レジスタを操作して前記ダイジェスト・データからデジタル署名を求めるための複数の署名専用命令を有する

ことを特徴とするセキュア・プロセッサ。

[2] 請求項1に記載のセキュア・プロセッサにおいて、

プロセッサの走行モードとして、一般モードとセキュリティ・モードを有し、

前記セキュリティ・モードを表示するセキュリティ・レジスタを備えるとともに、前記セキュリティ・モードをセットする一般命令及びリセットする署名専用命令を有し、

前記一般命令は一般モードのときに有効となり、前記署名専用命令はセキュリティ・モードのときに有効となることを特徴とするセキュア・プロセッサ。

[3] 請求項2に記載のセキュア・プロセッサにおいて、

前記セキュリティ・モード設定命令は、前記セキュリティ・レジスタをセットすると同時に、前記鍵カウンタを1023に初期設定し、

前記署名専用命令は、署名計算を鍵レジスタの1ビット分実行する命令の実行と同時に鍵カウンタをデクリメントして、順次ビットごとの署名計算が進行し、前記鍵カウンタが0のときのみにセキュリティ・モードをリセットすることを特徴とするセキュア・プロセッサ。

[4] (補正後) 請求項3に記載のセキュア・プロセッサにおいて、

前記ダイジェスト・レジスタに設定されたダイジェスト・データが16ビット毎に少なくと

も1つの1を有することを検出する手段を備え、

前記セキュリティ・モード設定命令は、16ビット毎に少なくとも1個は1があることを条件に、前記鍵カウンタを初期設定し、セキュリティ・レジスタがセットされたあとはダイジェスト・レジスタ内のデータは変更できないとすることを特徴とするセキュア・プロセッサ。

[5] 請求項3又は4に記載のセキュア・プロセッサにおいて、

セキュア・プロセッサには、主メモリに接続しており、

前記署名専用命令は、前記デジタル署名を求める演算の演算結果を、前記主メモリの特定の領域のみに格納して、デジタル署名演算の最終結果を前の演算結果に上書きすることを特徴とするセキュア・プロセッサ。

[6] 請求項1～5のいずれかに記載のセキュア・プロセッサを組み込んだICカード。